DAT621.FRD.

Pay-per-use communication device with double descrambling, in particular for television pictures

INSA1

The present invention pertains to the general field of the control of access to information such as television picture data. It relates more particularly to a pay-per-use communication device, with double descrambling.

In the case in particular of pay-per-use television, pay-per-use communication devices generally comprise a processing pathway receiving, at input, scrambled picture data, so as to deliver, at output, descrambled picture data, ready for direct use, for example for their viewing on a television or for their recording on a video recorder.

Such pay-per-use communication devices, which are known, comprise processing means capable of undertaking the descrambling of scrambled signals, with a view to their direct use, as well as an access control module conditioning the operation of these processing means.

Generally, the users hold memory cards each containing a user identifier associated with access entitlements to several pay-per-use television programmes, and each able to cooperate with an access control module of the aforesaid type. Now, the user of such a device is not currently able to view or record, on several televisions or recorders, the various programmes for which he nevertheless possesses access entitlements.

The only known current solution consists in providing two completely separate pay-per-use communication devices, with two separate access control modules, thereby raising the cost of such use and increasing its complexity, as well as the footprint to be allowed for.

The present invention aims to improve the situation.

It pertains to a device of the aforesaid type, comprising:

- a first input interface for receiving first scrambled signals, bearing first information subject to pay-per-use, in particular television pictures
- first processing means able to undertake the conversion of the first scrambled signals into first descrambled signals, capable of direct use,
- an access control module able to cooperate with a memory card comprising a user identifier associated with access entitlements, and conditioning the operation of the first processing means, and
- a first output interface for delivering the first descrambled signals with a view to direct use.

According to a general definition of the invention, the pay-per-use communication device further comprises:

- a second input interface for receiving second scrambled signals, bearing second information subject to pay-per-use and to which the said memory card is able furthermore to provide access entitlements,
- second processing means able to undertake the conversion of the second scrambled signals into second descrambled signals, capable of direct use, and
- a second output interface for delivering the second descrambled signals,

the access control module being able to cooperate with the memory card so as to condition the operation of the second processing means with a view to further allowing the conversion of the second scrambled signals.

Thus, the device according to the invention comprises a single access control module, cooperating with a single memory card holding access entitlements in respect of several television programmes, which may be viewed and/or recorded using two output interfaces each

linked, as the case may be, to means of direct use such as a television and a video recorder or two televisions, or else two video recorders.

According to an advantageous optional characteristic of the invention, the first and second processing means respectively comprise first and second management means for driving the respective conversions of the first and second scrambled signals. The first management means are arranged so as to talk to the access control module so as to activate the conversion of the first scrambled signals, whilst the second management means are preferably arranged so as to talk to the access control module by way of the first management means, with a view to activating the conversion of the second scrambled signals.

Advantageously, the first management means are arranged, on the one hand, to receive from the access control module, at predetermined time intervals, first and second control messages, for the respective conversions of the first and second scrambled signals, and, on the other hand, to transmit the said second control messages to the second management means.

Other advantages and characteristics of the present invention will become apparent on reading the detailed description hereinbelow and the appended drawings in which:

- Figure 1 diagrammatically represents a decoder device of the prior art;

- Figure 2 diagrammatically represents a decoder device according to the invention; and

- Figure 3 diagrammatically represents a preferred way of carrying out the dialogues by which the aforesaid

first and second management means talk to each other and to the access control module.

The detailed description hereinbelow and the appended drawings contain in essence elements of definite character. They may not only serve for better understanding of the present invention, but may also contribute to its definition, as the case may be.

Reference is firstly made to Figure 1 in order to describe a pay-per-use communication device of the prior art. In the example described, this involves a device for descrambling moving picture data for digital television, in particular of MEDIABOX (registered trademark) type and capable of descrambling programmes broadcast by CANALSATELLITE (registered trademark).

Such a device comprises an input interface E linked to an antenna AT able to communicate with a plurality of satellites. In the application to the descrambling of CANALSATELLITE programmes, the antenna AT receives radiofrequency waves transmitted by the ASTRA and EUTELSAT (registered trademarks) satellites. The polarizations of the radiofrequency waves transmitted by the satellites are here rectilinear. In particular, two types of polarization, horizontal and vertical, are provided for.

In the example represented in Figure 1, the antenna AT is of parabolic type. The input interface E of the descrambler device is linked to an LNB head (the abbreviation standing for "Low Noise Block"), suitable for converting the frequencies of the signals received with a view to their demodulation, generally on the basis of a local oscillator and advantageously with low phase noise. This LNB head is devised substantially at the focus 9 of the parabola.

The descrambler device comprises a pathway for processing the picture data received, which begins with a tuner 11 linked to the input interface E and for selecting a desired channel within the range of converted frequencies. This channel corresponds to a transmission programme to which the user of the descrambler has access and which he wishes to use for viewing or recording.

The output signal from the tuner 11 is then coherently demodulated (synchronous demodulation) by passing through a demodulation and error correction stage 12. In practice, slaving to the frequency and to the phase of the oscillator of the demodulation is performed using at least one phase lock loop.

In the example described, the scrambled picture data are in the MPEG2 format (the abbreviation standing for "Motion Picture Experts Group"), corresponding to a compression standard for moving pictures. The demodulation stage 12 furthermore comprises filtering and error correction modules, carrying out decodings known to the person skilled in the art such as a VITERBI decoding in the presence of a convolution code on transmission, a REED-SOLOMON decoding, etc. Reference may be made to the book by Hervé BENOIT : "*La télévision numérique*" [Digital television], ed. DUNOD, Paris, 1998, to find detailed elements relating to such decodings.

At the output of the demodulation/error correction stage 12, the signals feed into a demultiplexing block 13, allowing the selection, by means of chosen filters, of elementary trains signals in the form of packets in the MPEG2 format, corresponding to the programme chosen by the user. The demultiplexing block 13 is combined with a descrambler module 16 which carries out the selection and the descrambling of the packets of the chosen broadcast programme.

The descrambling module communicates with a main processor 10, in practice, via a parallel bus allowing fast transfer of data. An access control module 1, able to cooperate with a smart card CA, provides the processor 10 with a descrambling key, for example in the form of an access control message CW1 (control words), allowing the processor 10 to activate the descrambling module 16. In particular, the processor 10 talks to the access control module 1 by transmitting conditional access messages ECM1 (standing for "Entitlement Control Message") and/or EMM1 (standing for "Entitlement Management Message") and by receiving control messages CW1 (standing for "Control Word").

Descrambled MPEG packets emanating from the demultiplexing block 13 are then applied to an MPEG2 decoding block 14, which additionally carries out graphics screen generator functions, and in practice requires a dynamic random access memory 17 (DRAM). The signals emanating from the decoding block 14, which were initially converted into digital signals at the output of the demodulation block 12, are reconverted into analogue signals, by a video encoding block 15. The video and audio signals, thus made available for direct use from a television or video recorder (TV), are delivered to an output interface S of the descrambler device.

The assembly of blocks and modules of the processing pathway 11, 12, 13, 14, 15 and 16 is driven by the processor 10 which controls the links between modules, interprets the commands originating from a remote control (block referenced 3 in Figure 1), manages the smart card reader 1, as well as communication interfaces which are generally present, for example to a display device 4, a modem 5, a PC link to a computer 6, an entry keyboard 7 and/or a second interface 8 to a reader of a second smart card for other access entitlements, as the case may be. The processor 10 can

furthermore drive an interface 2, for example a serial link interface to a development station.

Thus, such a device in the prior art can only deliver descrambled picture data for a single channel, and to a single means of direct use (television only TV in the example represented in Figure 1).

Reference is now made to Figure 2 in order to describe a pay-per-use communication device according to the present invention.

As compared to the device represented in Figure 1, this device overall comprises two processing pathways in parallel. A mother pathway comprising the elements 11 to 16 (tuner, demodulation block, demultiplexing block, descrambling module, MPEG decoding block and video encoding block), cooperates with an access control module 1 which receives a descrambling key from a smart card CA. A processor 10 drives the elements of this mother pathway.

A second pathway (daughter pathway) comprises similar elements: a tuner 21, a demodulation and error correction block 22, an MPEG demultiplexing block 23 which cooperates with a descrambling module 26, an MPEG decoding block 24 and a video encoding block 25. On the other hand, the various elements of the second daughter pathway are driven by a second processor 20 which the descrambler device according to the invention comprises. This processor 20 is then arranged so as to cooperate with the processor 10 of the mother pathway, in particular so as to receive the descrambling key provided by the access control module 1. This descrambling key is transmitted to the descrambling module 26 of the daughter pathway and the two mother and daughter pathways can thus operate independently of one another, in respect of channel decoding with the aid of the tuners 11 and 21, in respect of the

demodulations and error corrections at 12 and 22, in respect of the MPEG demultiplexing at 13 and 23, the MPEG decoding at 14 and 24 and finally the video encoding at 15 and 25.

One of the advantages which the invention then affords is to provide two independent outputs (output interfaces S1 and S2), able to deliver picture data emanating from different channels corresponding to different programmes for which the user has an entitlement of access via the smart card CA. Thus, the user can simultaneously view a programme on a television TV and record a different programme using a video recorder MG, using a single memory card CA and a single access control module 1.

In the example described, the antenna AT can communicate with two satellites of the aforesaid type (ASTRA and EUTELSAT). Thus, a user might wish to view a programme broadcast by one satellite and to record a programme broadcast by the other satellite. The applicant thus found itself confronted with a difficulty relating to the receiving of programmes radio-broadcast by two different sources (satellites).

Advantageously, the focus 9 of the parabolic antenna AT then comprises four LNB heads, linked to the input E of the device according to the invention:

- two heads for respective horizontal and vertical polarizations of radiofrequency waves originating from the ASTRA satellite and

- two heads for respective horizontal and vertical polarizations of radiofrequency waves originating from the EUTELSAT satellite.

Preferably, the processor 10 from the mother pathway transmits to the processor of the daughter pathway 20

the descrambling key which it gleans from the access control module 1, with a view to activating the descrambling module 26 of the daughter pathway. Thus, the processor 20 drives only the conversion operations (demodulation, demultiplexing, descrambling, MPEG decoding/video encoding) performed by the daughter pathway, and then exhibits a restricted number of applications as compared with the processor 10.

Reference is now made to Figure 3 in order to describe the dialogue in which the processor 10 of the mother pathway talks to the processor 20 of the daughter pathway, on the one hand, and to the access control module 1, on the other hand.

At the output of the demultiplexing block 13 of the mother pathway, the processor 10 receives signals bearing information relating to predetermined access conditions. These signals, initially contained in the multiplexed packets U0 entering the demultiplexing block 13, are interpreted and shaped by the processor 10 which then delivers the aforesaid conditional access messages ECM1 and EMM1.

In parallel with this, at the output of the demultiplexing block 23 of the daughter pathway, the processor 20 receives signals bearing information relating to predetermined access conditions. These signals, initially contained in the multiplexed packets V0 entering the demultiplexing block 23, are interpreted and shaped by the processor 20 which then delivers the aforesaid conditional access messages ECM2 and EMM2.

The processor 20 of the daughter pathway delivers the messages ECM2 and EMM2 to the processor 10 of the mother pathway. The processor 10 of the mother pathway delivers the messages ECM1 and EMM1, as well as the

messages ECM2 and EMM2 of the processor 20, to the access control module 1.

The memory of the smart card CA contains a key for descrambling programmes which the two processing pathways are able to descramble. The access control module 1 interprets this descrambling key and transmits two sets of control words CW1 and CW2 to the processor 10 of the mother pathway, the sets being intended for the descramblings of the signals passing respectively through the mother pathway and the daughter pathway. Preferably, the control words CW1 and CW2 are symmetric-key cryptographic functions and advantageously depend on a single descrambling key K, on the one hand, and on associated control messages on the other hand, respectively ECM1, EMM1 and ECM2, EMM2.

In practice, these control words are transmitted to the processor 10 at regular time intervals, typically every five seconds, or else every two seconds. The processor 10 in turn transmits the control words CW2 to the processor 20 of the daughter pathway.

The processor 10 of the mother pathway, upon receipt of the control words CW1, activates the descrambling module 16 so as to deliver signals bearing descrambled picture data U1. For the daughter pathway, the processor 20, on receipt of the control words CW2, activates the descrambling module 26 so as to deliver signals bearing descrambled picture data V1.

Thus, the processor 10 shapes the conditional access messages ECM1 and EMM1, receives its conditional access messages ECM2 and EMM2 from the processor 20 and interrogates the access control module 1. In return, the access control module 1 delivers the control words CW1 and CW2 to the processor 10. The processor 10 activates or otherwise, depending on the words CW1, the descrambling module 16 of the mother pathway. According

to a protocol of the master/slave type, the processor 10 (master) talks to the processor 20 (slave) by transmitting to the latter the control words CW2, so as to activate or otherwise, depending on the words CW, the descrambling module 26 of the daughter pathway.

More particularly, the processor 10 manages the sequential dispatching of the messages ECM1, ECM2, EMM1 and EMM2, as well as of the messages relating to the programmes viewed and/or recorded, to the access control module 1, and in return receives the control words CW1 and CW2 which it sorts for dispatch to the descrambler module 16 and to the processor 20.

The processor 10 of the mother pathway thus drives the elements 11 to 16 of this processing pathway, as well as the memory 17 comprising for example software of "MEDIAHIGHWAY" type (registered trademark) so as to manage the operational protocol (demodulation, error correction, MPEG demultiplexing, descrambling, MPEG decoding and video encoding), and/or software of the "MEDIAGUARD" type (registered trademark) for talking to the "Canalsatellite" subscription card CA, with which the processor 10 manages the descrambling keys, both in respect of the programme viewed and of the programme to be recorded. In particular, new versions of these items of software are envisaged in respect of the device according to the invention, furthermore affording the master processor 10 the function of managing the slave processor 20 according to a protocol of master/slave type, as well as optional functions such as authorization to record a different programme from that viewed, start and stop recording control, etc.

The processor 10 of the mother pathway in the device according to the invention furthermore carries out the management of the peripheral links 2 to 8. In particular, an infrared programmer may be provided at the output S2 of the daughter pathway (recording

pathway in the example), driven by the processor 10 with a view to programming the video recorder MG directly.

Of course, the present invention is not limited to the implementation described hereinabove by way of example. It extends to other variants.

It will thus be understood that the output S2 may be linked to a second television, if, in a household, users possessing access entitlements wish to view two different programmes. In particular, provision may be made to remodulate the audio/video signals at the output of the encoding block 25 (output interface S2), for transmission by coaxial cable to the second television.

Furthermore, provision may be made for two outputs, S1 and S2, to one and the same television, if one wishes, in particular, to view two programmes simultaneously, for example, on a split display screen (mosaic). In particular, the device according to the invention can comprise a plurality of daughter processing pathways whose slave processors talk to a master processor of a mother pathway, according to a master/slave protocol of the type described hereinabove.

The link of the input interfaces E1 and E2 of the device described hereinabove to a parabolic antenna AT is described here by way of example. As a variant, this link may be effected by cable, or over the airwaves.

The moving picture data compression format, of MPEG2 type, is described hereinabove by way of example. As a variant, this format may also be of MPEG1 type, of MPEG4 type (more recent version), or some other type.

The invention applies, of course, to any type of access control pay-per-use communication device, allowing the

viewing of programmes other than those broadcast by "Canalsatellite". In general, it applies to a device comprising twinned means for processing scrambled signals, possibly bearing information other than picture data.

Finally, the various peripheral links 2 to 8 represented in Figures 1 and 2 are described hereinabove by way of examples. They may be varied, depending on the applications envisaged. More generally, the architecture of the processing protocols described hereinabove is illustrated by way of example. In particular, the tasks incumbent respectively on the processors 10 and 20 may vary.